8Б

УДК 519.711/.72

***А.Я. Белецкий, А.А. Белецкий, Д.А. Стеценко***
Национальный авиационный университет МОН Украины, г. Киев, Украина
abelnau@ukr.net

# Модифицированный матричный асимметричный криптографический алгоритм Диффи – Хэллмана

В статье рассматривается проблема построения систем распределения ключей шифрования между абонентами компьютерной сети по открытым каналам связи. В основу системы положен модифицированный асимметричный криптографический алгоритм Диффи – Хэллмана (DH). Суть модификации сводится к замене больших простых чисел алгоритма DH гарантированно невырожденными *n*-полными двоичными матрицами высокого порядка. Предлагаются методы синтеза таких матриц.

## Введение

Толчком к развитию криптографических систем с открытым ключом (асимметричное шифрование, асимметричный шифр, также именуемые шифрами с открытым ключом) послужило опубликование в 1976 году знаменитой статьи У. Диффи и Р. Хэллмана «Новые направления в криптографии» [1]. Разработанный впоследствии алгоритм Диффи – Хэллмана (Diffie – Hellman, DH) позволял двум сторонам получить общий секретный ключ, используя незащищенный канал связи. Структурная схема классического DH-алгоритма показана на рис. 1.

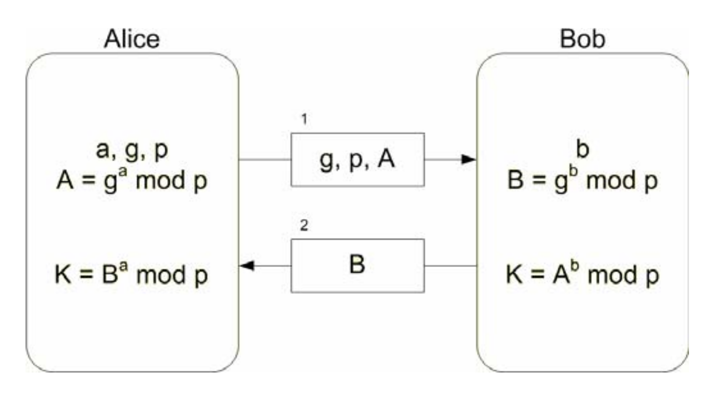



Рисунок 1 – Структурная схема протокола обмена ключами Диффи – Хэллмана

Предполагается, что один из общающихся между собой абонентов, назовем их Алиса и Боб, вырабатывает достаточное большое (несколько Кбит) двоичное простое число $p$ и вычисляет образующий (примитивный) элемент $g$ циклической абелевой группы над $p$. Числа $p$ и $g$ являются открытыми (публичными) ключами протокола DH, которые могут быть известны также другим заинтересованным лицам. Для того чтобы создать неизвестный более никому секретный ключ $K$, оба абонента генерируют большие случайные числа: первый абонент (Алиса) – число $a$, второй абонент (Боб) число $b$. Затем первый абонент вычисляет значение $A = g^a \bmod p$ и пересылает его второму, а второй вычисляет $B = g^b \bmod p$ и передаёт первому. На втором этапе первый абонент на основе имеющегося у него числа $a$ и полученного по сети $B$ вычисляет

значение $B^a \bmod p = g^{ab} \bmod p$, а второй абонент на основе имеющегося у него $b$ и полученного по сети $A$ вычисляет значение $A^b \bmod p = g^{ab} \bmod p$. Как нетрудно видеть, у обоих абонентов получилось одно и то же число: $K = g^{ab} \bmod p$. Его они и могут использовать в качестве секретного ключа, поскольку здесь злоумышленник встретится с практически неразрешимой (за разумное время) проблемой вычисления $g^{ab} \bmod p$ по перехваченным числам $g^a \bmod p$ и $g^b \bmod p$, если числа $p$, $a$, $b$ выбраны достаточно большими.

Однако DH-алгоритм формирования секретного ключа шифрования, будучи уязвимым к атакам типа «человек посередине», не решал проблему аутентификации. Без дополнительных средств ни один из пользователей не мог быть уверен, что он обменялся ключами именно с тем пользователем, который ему был нужен. Годом позже был предложен алгоритм асимметричного шифрования RSA, который решил проблему общения через незащищённый канал [2]. RSA стал первым асимметричным алгоритмом, пригодным как для шифрования, так и для цифровой подписи. Цифровая подпись обеспечивает не только аутентификацию автора сообщения, отсутствовавшую в DH-шифре, но и подтверждение целостности содержимого подписанного сообщения.

Алгоритмы DH и RSA используются в большом числе криптографических приложений. И тем ни менее данным алгоритмам присущ ряд существенных недостатков, сужающих области их применения. Среди этих недостатков отметим, по крайней мере, следующие. Во-первых, поименованные шифраторы базируются на использовании больших простых чисел, длина которых может превышать несколько Кбит. Генерация таких чисел представляет собой достаточно сложную задачу, причем их простота обеспечивается с конечной вероятностью, не достигающей единицы. Во-вторых, скорость шифрования асимметричными алгоритмами на несколько порядков (три и более) ниже скорости шифрования в симметричных криптосистемах. Поэтому, и прежде всего в силу второго указанного недостатка, асимметричные алгоритмы применяются в основном в системах обмена ключами в многопользовательских корпоративных компьютерных сетях.

В ряде работ российских ученых [3], [4] предлагается строить блочные шифры на основе обратимых матриц над полем $GF(2)$. Если $\boldsymbol{X}, \boldsymbol{Y}$ – векторы, представляющие соответственно открытый и зашифрованный тексты, а $\boldsymbol{M}$ – шифрующая матрица, то зашифрование задается уравнением, $\boldsymbol{Y} = \boldsymbol{M} \cdot \boldsymbol{X}$, а расшифрование – уравнением $\boldsymbol{X} = \boldsymbol{M}^{-1} \cdot \boldsymbol{Y}$. Для установления сеансовых ключей в системе авторы предлагают использовать протокол Диффи – Хэллмана в циклической группе матриц $\langle \boldsymbol{M} \rangle$, где матрица $\boldsymbol{M}$ считается общедоступной. При этом пользователь $A$ вырабатывает случайный показатель $x$, вычисляет матрицу $\boldsymbol{M}^x$ и посылает ее пользователю $B$. Пользователь $B$ вырабатывает случайный показатель $y$, вычисляет матрицу $\boldsymbol{M}^y$ и посылает пользователю $A$. Затем оба пользователя возводят полученные матрицы в свои степени и получают общую секретную матрицу (ключ) $\boldsymbol{M}^{xy} = \boldsymbol{M}^{yx}$, являющуюся неизвестной для неаккредитованного абонента. Поскольку число $N$ невырожденных матриц велико (приводится оценка $N = 2^{n^2-2}$, где $n$ – порядок квадратной двоичной матрицы), авторы утверждают, что вычисление ключа имеет переборную сложность.

Вслед за упомянутыми работами появилась статья [5], в которой многие утверждения, содержащиеся в [3], опровергаются или ставятся под сомнение. В частности, в [5] доказывается, что в том виде, в котором в [3] предлагается строить матричное шифрование DH, не обеспечивает обещанного уровня криптостойкости, а ключ зашифрования $\boldsymbol{M}^{xy}$ легко взламывается.

**Целью данной статьи** является, во-первых, разработка матричного алгоритма распределения ключей шифрования, модифицирующего известную асимметричную схему Диффи – Хэллмана, между аккредитованными абонентами многопользовательской

компьютерной сети, устраняющего основные замечания к подобным алгоритмам, высказанным в работе [5]. И, во-вторых, синтез гарантированно невырожденных двоичных матриц, используемых в модифицированном шифраторе DH, последовательность степеней которых в кольце вычетов по mod 2 образует последовательность максимальной длины (*m*-последовательность).

# Синтез матричного криптоалгоритма Диффи – Хэллмана

Обобщенная структурная схема модифицированного алгоритма (криптопримитива) Даффи – Хэлмана приведена на рис. 2.

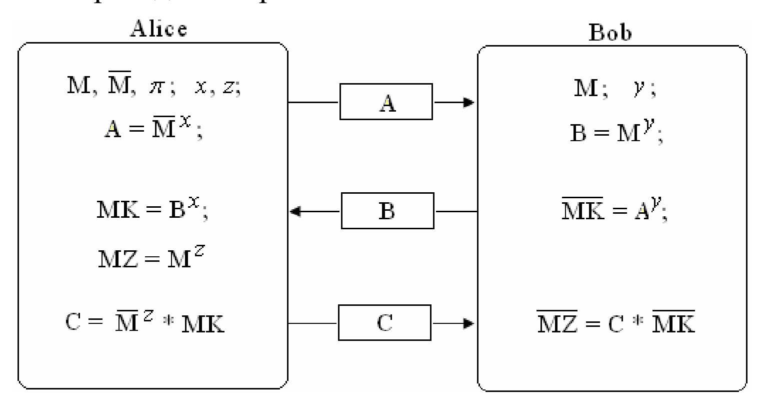



Рисунок 2 – Модифицированный матричный DH-алгоритм шифрования данных

Суть работы модифицированного алгоритма шифрования сводится к следующему. Абоненты Алиса ($\mathcal{A}$) и Боб ($\mathcal{B}$) выбирают двоичные достаточно большого порядка *n*-полные прямую $\boldsymbol{M}$ и обратную $\overline{\boldsymbol{M}}$ матрицы (способ их формирования изложен ниже). Эти матрицы могут быть общедоступными. Независимо друг от друга абоненты $\mathcal{A}$ и $\mathcal{B}$ вырабатывают секретные случайные числа $x$ и $y$ соответственно. Рекомендуемый порядок векторов $x$ и $y$ должен составлять величину, вдвое меньшую порядка шифрующих матриц. Абонент $\mathcal{A}$ вычисляет матрицу $\boldsymbol{A} = \overline{\boldsymbol{M}}^{x}$ и посылает ее Бобу, который, в свою очередь, вычисляет матрицу $\boldsymbol{B} = \boldsymbol{M}^{y}$ и посылает ее Алисе. Далее каждый из абонентов $\mathcal{A}$ и $\mathcal{B}$ возводит полученные матрицы в свои секретные степени $x$ и $y$. В результате выполненных операций Алиса приобретает секретную матрицу зашифрования $\boldsymbol{MK} = \boldsymbol{B}^{x} = \boldsymbol{M}^{xy}$, а Боб – матрицу расшифрования $\overline{\boldsymbol{MK}} = \boldsymbol{A}^{y} = \overline{\boldsymbol{M}}^{xy}$.

С целью противодействия атаке типа «человек посередине» в модифицированном DH-алгоритме предлагаются такие меры. Как известно, в системах криптографической защиты данных желательно не допускать легко устанавливаемой зависимости между последовательно используемыми ключами (в рассматриваемом алгоритме – матрицами) шифрования. С этой целью представляется целесообразным обновлять матрицы шифрования $\boldsymbol{MK}$ после некоторого фиксированного или согласованного между абонентами $\mathcal{A}$ и $\mathcal{B}$ вариативного периода (сеанса) передачи данных по правилу $\boldsymbol{MK} = \boldsymbol{MK} \cdot \boldsymbol{MZ}$, где $\boldsymbol{MZ} = \boldsymbol{M}^{z}$, причем $z$ – секретное случайное натуральное число, вырабатываемое абонентом $\mathcal{A}$. Аналогично осуществляется модификация матрицы расшифрования $\overline{\boldsymbol{MK}}$. В рассматриваемом алгоритме шифрование данных осуществляется блоками, размер которых совпадает с числом элементов шифрующих матриц. Предположим, что Алиса и Боб договорились о том, что после $k$ сеансов передачи блоков данных в очередном $(k+1)$-м сеансе Алиса передает матрицу $\boldsymbol{C}$ (рис. 2). Боб извлекает из блока $\boldsymbol{C}$ матрицу

$\overline{\boldsymbol{MK}}$. Начиная с $(k+2)$-го сеанса связи, Алиса и Боб переходят на обновленные матрицы шифрования данных. Первые $k$ блоков передачи информации от абонента $\mathcal{A}$ к $\mathcal{B}$ могут содержать нейтральный (несекретный) текст. На $(k+1)$-м раунде (сеансе) связи абоненты переходят на новый ключ шифрования. Первым после смены ключа шифрования передается блок, содержащий специальные данные, расшифровка которых на приемном конце позволяет однозначно идентифицировать наличие или отсутствие «человека посередине». Если таковой обнаружен, дальнейшая передача информации прерывается, и тем самым противник лишается доступа к секретной информации. Компрометация «человека посередине» обусловлена следующими причинами. Естественно предположить, что противник подменяет текст Алисы собственным текстом, в результате чего на $k$-м шаге передачи данных Боб получает искаженную матрицу $\overline{\boldsymbol{MZ}}$. Поэтому он оказывается не в состоянии расшифровать специальный блок и информирует Алису о прекращении связи.

# Синтез шифрующих матриц

Одной из важных проблем, которая возникает в ходе реализации предлагаемого алгоритма DH, является формирование шифрующих $n$-полных матриц $\boldsymbol{M}$. В монографии [6] разработана методика формирования матриц преобразования, отвечающих обобщенным (составным) кодам Грея (КГ). Составным кодом Грея (СКГ) называется код $\boldsymbol{G}$, образованный произведением простых (элементарных) кодов Грея. Полное множество простых КГ включает шесть кодов, сведенных в табл. 1. В их число входят так называемые инварианты преобразования Грея, которые включают единичную матрицу и матрицу инверсной перестановки, а также операторы прямого и обратного как лево-, так и правостороннего преобразований Грея (ПГ). Перечисленным элементарным операторам (кодам) Грея поставим в соответствие символьные обозначения $\boldsymbol{g}_i$, $i=\overline{0,5}$. Для простоты обозначения вместо символов кодов будем использовать также их цифровые индексы.

Таблица 1 – Полная группа простых операторов Грея

| Обозначение оператора | Выполняемая операция | Аббревиатура оператора |
|---|---|---|
| $e$ (или 0) | Сохранение исходной комбинации | – |
| 1 | Инверсная перестановка | ИП |
| 2 | Прямое кодирование по Грею левостороннее | $\overset{\circ\rightarrow}{\text{КГ}}$ |
| 3 | Обратное кодирование по Грею левостороннее | $\overset{\circ\rightarrow}{\text{ОКГ}}$ |
| 4 | Прямое кодирование по Грею правостороннее | $\overset{\leftarrow\circ}{\text{КГ}}$ |
| 5 | Обратное кодирование по Грею правостороннее | $\overset{\leftarrow\circ}{\text{ОКГ}}$ |

Приведем матричные формы простых операторов Грея, отвечающих прямому $\boldsymbol{g}_2$ и обратному $\boldsymbol{g}_3$ левостороннему КГ четвертого порядка:

$$2=\boldsymbol{g}_2=\begin{bmatrix}1&1&0&0\\0&1&1&0\\0&0&1&1\\0&0&0&1\end{bmatrix};\ 3=\boldsymbol{g}_3=\begin{bmatrix}1&1&1&1\\0&1&1&1\\0&0&1&1\\0&0&0&1\end{bmatrix}.$$

Операторы правосторонних ПГ (прямого $\boldsymbol{g}_4$ и обратного $\boldsymbol{g}_5$) образуются транспонированием соответствующих операторов левосторонних ПГ, т.е. $\boldsymbol{g}_4 = \boldsymbol{g}_2^{\mathrm{T}}$ и $\boldsymbol{g}_5 = \boldsymbol{g}_3^{\mathrm{T}}$. Кроме перечисленных операторов в полную группу простых ПГ, как отмечено выше, входят также единичная матрица $(\boldsymbol{g}_0)$ и матрица инверсной перестановки $(\boldsymbol{g}_1)$, в которой на элементах вспомогательной диагонали находятся единицы, а на остальных элементах – нули.

Аналитически СКГ можно представить произведением

$$\boldsymbol{G} = \prod_{j=1}^{k} \mathbf{g}_j ,$$

где $\boldsymbol{g}_j$ – простой КГ, выбираемый из полной группы $\{\overline{\boldsymbol{g}_0, \boldsymbol{g}_5}\}$, а $k$ – порядок СКГ.

Как простые, так и составные КГ обладают рядом замечательных свойств. Во-первых, отвечающие им матрицы преобразования являются невырожденными и в силу этого оказываются обратимыми. И, во-вторых, поскольку любой КГ является образующим элементом абелевой циклической группы, то существуют достаточно простые алгоритмы обращения СКГ.

Подтвердим последнее утверждение на простом примере. Пусть $n = 4$ и $\mathbf{G} = 4251$. Выбранному СКГ отвечает матрица преобразования

$$\boldsymbol{G} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}. \quad (1)$$

Пусть, кроме того, задана степень $k = 2$ матрицы $\boldsymbol{G}$. Согласно (1) имеем

$$\boldsymbol{G}^2 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}. \quad (2)$$

В общем случае для вычисления обратной матрицы $k$-й степени образующего элемента $\boldsymbol{G}$ циклической группы $L$-го порядка можно воспользоваться, по крайней мере, тремя способами. Поскольку $\boldsymbol{G}^L \equiv \boldsymbol{E}$, то:

Вариант 1. $\overline{\boldsymbol{G}^k} = \boldsymbol{G}^{L-k}$;

Вариант 2. $\overline{\boldsymbol{G}^k} = \boldsymbol{G}^k \cdot \boldsymbol{G}^{L-2k}$.

Порядок циклической группы $L$, порождаемой элементом $\boldsymbol{G}$ в (1), равен семи. Это означает, что $\boldsymbol{G}^7 = \boldsymbol{E}$. Каждый из приведенных выше вариантов оценок обратной матрицы приводит к одинаковому результату

$$\overline{\boldsymbol{G}^2} = \boldsymbol{G}^5 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}. \quad (3)$$

Корректность выражения (3) легко проверить, перемножив матрицы прямого (2) и обратного (3) преобразований. Получим единичную матрицу, как и должно быть.

Можно воспользоваться еще одним (третьим, но далеко не последним) вариантом обращения СКГ. Он состоит их двух этапов. На первом этапе символическая запись кода переписывается в обратном порядке. На втором этапе каждый простой КГ заменяется соответствующим ему обратным кодом. Например, если $\boldsymbol{G} = 24135$, то $\overline{\boldsymbol{G}} = 42153$. В самом деле

$$\boldsymbol{G} \cdot \overline{\boldsymbol{G}} = 241\overline{3\underline{5 \cdot 4}2}153 = \boldsymbol{E}\,. \qquad (4)$$

В конструкции (4) симметрично относительно знака умножения находятся взаимно обратные простые коды (две пары таких кодов выделены связующими линиями), произведение которых равно единичной матрице. И, следовательно, полное произведение множителей в средней части выражения (5) также равно $\boldsymbol{E}$, что и подтверждает корректность определения обратного СКГ по третьему варианту.

Как оказалось, приемлемыми для криптографических приложений являются матрицы, отвечающие СКГ типа 1$\boldsymbol{g}$, где $\boldsymbol{g} = \overline{2,5}$ есть простые операторы Грея. Замечательная особенность таких матриц состоит в том, что порядок $L_n$ циклических групп, порождаемых операторами 1$\boldsymbol{g}$, за небольшим исключением (названных нами артефактом), определяется соотношением:

$$L_n = 2^m - 1, \quad m \le n\,, \qquad (5)$$

где $n$ – порядок матрицы.

В табл. 2 приведены оценки $L_n$, полученные прямыми компьютерными вычислениями.

Таблица 2 – Порядок циклических групп, отвечающих СКГ $\boldsymbol{G} = 1\mathbf{g}$

| $n$ | $L_n$ | $n$ | $L_n$ | $n$ | $L_n$ | $n$ | $L_n$ |
|---|---|---|---|---|---|---|---|
| | | 9 | $2^9-1$ | 17 | $2^{12}-1$ | 25 | $2^8-1$ |
| 2 | $2^2-1$ | 10 | $2^6-1$ | 18 | 87381 | 26 | $2^{26}-1$ |
| 3 | $2^3-1$ | 11 | $2^{11}-1$ | 19 | $2^{12}-1$ | 27 | $2^{20}-1$ |
| 4 | $2^3-1$ | 12 | $2^{10}-1$ | 20 | $2^{10}-1$ | 28 | $2^9-1$ |
| 5 | $2^5-1$ | 13 | $2^9-1$ | 21 | $2^7-1$ | 29 | $2^{29}-1$ |
| 6 | $2^6-1$ | 14 | $2^{14}-1$ | 22 | $2^{12}-1$ | 30 | $2^{30}-1$ |
| 7 | $2^4-1$ | 15 | $2^5-1$ | 23 | $2^{23}-1$ | 31 | $2^6-1$ |
| 8 | $2^4-1$ | 16 | $2^5-1$ | 24 | $2^{21}-1$ | 32 | $2^6-1$ |

Из анализа данных, представленных в табл. 2, приходим к таким выводам:

Во-первых, подтверждается форма оценки $L_n$, заданная соотношением (5). Исключение (артефакт) проявляется лишь в точке $n = 18$, в которой $L = 87381_{10} = 10101010101010101_2 = (2^{18}-1)/3$. Попробуем разобраться более подробно с отмеченным «недоразумением». Двоичный эквивалент десятичного числа $2^{18}-1$ представляет собой последовательность из 18 единичек. Умножив двоичный вектор $L$ на три, как раз и получим значение $L_{18} = 2^{18}-1$. Таким образом, на числовом отрезке длиной $2^{18}-1$ укладывается три интервала периода $L = 87\,381$. А это означает, что как степень 87 381, так и степень $2^{18}-1$ обращают $\boldsymbol{M}$ в единичную матрицу. Этим и объясняется появление артефакта.

Во-вторых, существуют такие значения порядка $n$ (в табл. 1 они выделены затенением), для которых элементы циклических групп, порождаемые степенями

матриц $\boldsymbol{M}$ в кольце вычетов по mod 2, составляют последовательность максимальной длины, равную $2^n - 1$ (так называемые числа Марсена), т.е.

$$L_n = 2^n - 1, \tag{6}$$

где $n$ – порядок матрицы.

Матрицы $\boldsymbol{M}$, период цикла которых удовлетворяет условию (6), будем называть *n-полными.* Приведем ряд других примеров последовательностей, которые можно назвать *n*-полными. Такой является последовательность *n*-битных двоичных чисел (исключая нуль), или последовательность элементов расширенного поля Галуа $GF(2^n)$ без нулевого элемента и т.д.

Одним из важнейших результатов, к которому мы приходим на основании анализа табл. 2, состоит в том, что период цикла группы 1***g*** представляет собой *степенную величину*. Это обстоятельство, во-первых, дает нам возможность существенно сократить затраты машинного времени, необходимые для вычисления оценок $L_n$. И, во-вторых, наталкивает на мысль о целесообразности поиска других выражений для СКГ (отличных от 1***g***), которые порождают *n*-полные матрицы $\boldsymbol{M}$ *n*-го порядка. И такие СКГ были найдены. Часть из них представлена в табл. 3.

Таблица 3 – Составные коды Грея, доставляющие двоичным матрицам *n*-го порядка свойство *m*-полноты

| Порядок матрицы (*n*) | | | |
|---|---|---|---|
| 32 | 64 | 128 | 256 |
| 244424 | 22533435 | 2425535 | 24334225 |
| 2442224 | 22534335 | 2433534 | 25224334 |
| 12242253 | 24334225 | 2435334 | 2222535224 |
| 12242443 | 25224334 | 22524224 | |

Пусть $\boldsymbol{M}$ есть *n*-полная двоичная матрица *n*-го порядка, отвечающая СКГ $\boldsymbol{G}$. Относительно *n*-полных матриц $\boldsymbol{M}$ доказано следующее утверждение.

**Утверждение.** *n-полнота матриц* $\boldsymbol{M}$ *инвариантна к группам линейных преобразований* $\boldsymbol{\Omega}$ *над СКГ* $\boldsymbol{G}$ *и преобразований* $\boldsymbol{Q}$ *над строками и столбцами матриц* $\boldsymbol{M}$.

В состав $\boldsymbol{\Omega}$-группы входят такие операторы линейных преобразований над $\boldsymbol{G}$: циклического сдвига, обращения, инверсии и сопряжения, а также произвольные комбинации этих операторов.

Кратко поясним суть преобразований, входящих в вышеперечисленные группы. Введем (табл. 4) символику для операторов, входящих в $\boldsymbol{\Omega}$-группу преобразований.

Таблица 4 – Символическое обозначение операторов преобразования

| Обозначение оператора | Тип преобразования |
|---|---|
| $\overrightarrow{1}_k$, $\overleftarrow{1}_k$ | Циклический сдвиг |
| 2 | Обращение |
| 3 | Инверсия |
| 4 | Сопряжение |

Стрелки оператора циклического сдвига указывают направление прокрутки СКГ $\boldsymbol{G}$, а нижний индекс $k$ – задает число разрядов сдвига. Например, $\overleftarrow{1}_3$ означает, что СКГ подвергается циклической прокрутке по часовой стрелке на три разряда (символа) кода. Обозначим через $\boldsymbol{G}$ в общем случае составной оператор преобразования. Например, $\boldsymbol{P} = 3$, или $\boldsymbol{P} = 2 \cdot \overrightarrow{1}_2$ и т.д., а преобразования над $\boldsymbol{G}$ будем записывать в виде $\boldsymbol{P}\{\boldsymbol{G}\}$.

Предположим, что некая $n$-полная матрица $n$-го порядка $\boldsymbol{M}$ образована составным кодом $\boldsymbol{G} = 25224334$ (значение взято из табл. 4). Фактически СКГ отвечает произведению (в кольце вычетов по mod 2) двоичных матриц $n$-го порядка. Это означает, правила преобразования СКГ $\boldsymbol{G}$ совпадают с общими правилами преобразования над произведением матриц. Сведем в табл. 5 результаты простых преобразований $\boldsymbol{P}$ над этим произведением.

Таблица 5 – Пример преобразований

| Оператор преобразования | Результат преобразования |
|---|---|
| $\overleftarrow{1}_2$ | 22433425 |
| 2 | 52253343 |
| 3 | 43342252 |
| 4 | 25524434 |

В частности, $\overrightarrow{1}_3\, 4\{25224334\} = 55244342$ и т.д.

$\boldsymbol{Q}$-группу линейных преобразований над $n$-полными матрицами $\boldsymbol{M}$ составляют операторы «дружной перестановки» строк и столбцов матрицы, частным случаем которых являются операторы «дружного циклического сдвига» строк и столбцов матрицы $\boldsymbol{M}$.

Проиллюстрируем «дружную перестановку» строк и столбцов на примере матрицы $\boldsymbol{M}$ шестого порядка, сформированной СКГ $\boldsymbol{G}$ = 12 435. Для удобства отобразим исходную матрицу в виде табл. 6. Выбрав «дружную перестановку» $\pi = 204153$, приходим к матрице, показанной в табл. 7.

Таблица 6 – Исходная матрица

| | | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| 0 | | 1 | 1 | 1 | 1 | 1 | 0 |
| 1 | | 0 | 0 | 0 | 0 | 1 | 0 |
| 2 | | 0 | 0 | 0 | 1 | 0 | 0 |
| 3 | | 0 | 0 | 1 | 0 | 0 | 0 |
| 4 | | 0 | 1 | 0 | 0 | 0 | 0 |
| 5 | | 1 | 1 | 0 | 1 | 0 | 1 |

Таблица 7 – «Дружная перестановка» строк и столбцов исходной матрицы

| | | 2 | 0 | 4 | 1 | 5 | 3 |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| 2 | | 0 | 0 | 0 | 0 | 0 | 1 |
| 0 | | 1 | 1 | 1 | 1 | 0 | 1 |
| 4 | | 0 | 0 | 0 | 1 | 0 | 0 |
| 1 | | 0 | 0 | 1 | 0 | 0 | 0 |
| 5 | | 0 | 1 | 0 | 1 | 1 | 1 |
| 3 | | 1 | 0 | 0 | 0 | 0 | 0 |

Исходная матрица, как и матрица, образованная «дружной перестановкой» ее строк и столбцов (не имеет значения, как организована дружная перестановка: сначала по столбцам, а потом по строкам, или наоборот) являются порождающими элементами циклических групп одинакового порядка.

# Выводы

1. Кроме обмена ключами шифрования по открытым каналам связи матричный DH-алгоритм может быть использован также в качестве линейного криптографического примитива. Естественно, что он не доставляет требуемого уровня статистических свойств шифрограммы, как и любой одиночный криптопримитив.

2. Целесообразность применения в криптографии матриц, отвечающих составным кодам Грея, объясняется рядом замечательных свойств, которыми они обладают. Во-первых, матрицы, порождаемые СКГ любого порядка, чрезвычайно просто генерировать. Во-вторых, такие матрицы являются гарантированно невырожденными. В-третьих, для них легко вычисляются обратные матрицы. И, наконец, отметим еще одну особенность. Как установлено на основании компьютерного моделирования, для произвольных порядков $n$ матриц существуют такие СКГ, которые доставляют соответствующим матрицам свойство $n$-полноты. Это свойство проявляется в том, что порядок циклических групп, формируемых этими матрицами, достигает максимального значения, равного $2^n - 1$.

# Литература


1. Diffie W. New Directions in Cryptography / W. Diffie, M.E. Hellman // IEEE Transactions on Information Theory. – 1976. – V. IT-22, № 6. – P. 644-654.
2. Коутинхо С. Введение в теорию чисел. Алгоритм RSA / Коутинхо С. – М. : Постмаркет, 2001. – 318 с.
3. Ерош И.Л. Адресная передача сообщений с использованием матриц над полем GF(2) / И.Л. Ерош, В.В. Скуратов // Проблемы информационной безопасности. – 2004. – № 1. – С. 72-78.
4. Ерош И.Л. Скоростное шифрование разнородных сообщений / И.Л. Ерош, М.Б. Сергеев // Вопросы передачи и защиты информации : сборник статей. – СПб. : СПб ГУАП, 2006. – С. 133-155.
5. Ростовцев А.Г. О матричном шифровании (криптика криптосистемы Ероша и Скуратова) [Электронный ресурс] / А.Г. Ростовцев. – Режим доступа : www.ssl.stu.neva.ru/psw/crypto/ rostovtsev/Erosh_Skuratov.pdf
6. Белецкий А.Я. Преобразования Грея : монография в двух томах / Белецкий А.Я., Белецкий А.А., Белецкий Е.А. – К. : Книжное изд-во НАУ, 2007. – Т. 1. Основы теории. – 412 с. ; Т. 2. Прикладные аспекты. – 644 с.


***А.Я. Білецький, А.А. Білецький, Д.А. Стеценко***

**Модифікований матричний асиметричний криптографічний алгоритм Діффі – Хеллмана**

У статті розглядається проблема побудови систем розподілу ключів шифрування між абонентами комп'ютерної мережі по відкритих каналах зв'язку. В основу системи покладений модифікований асиметричний криптографічний алгоритм Діффі – Хеллмана (DH). Суть модифікації зводиться до заміни великих простих чисел алгоритму DH гарантовано невиродженими *n*-повними двійковими матрицями високого порядку. Пропонуються методи синтезу таких матриць.

***A.Y. Beletsky, A.A. Beletsky, D.A. Stetsenko***

**Modified Matrix Asymmetric Encryption Diffie-Hellman**

The paper addresses the problem of constructing distribution of encryption keys between subscribers multiplayer network to open channels of communication. Based system the modified-HYDRATED asymmetric encryption algorithm Diffie-Hellman (DH). The essence of the modification is to replace large prime numbers algorithm DH guaranteed nondegenerate n - full binary matrices of high order. The methods of synthesis of such matrices.

*Статья поступила в редакцию 13.07.2010.*